REMARKS

To date, the Examiner has not indicated that the subject matter of the information disclosure statement (IDS) filed July 14, 2005 has been properly considered. A copy of such IDS is submitted herewith. If the Examiner requires additional copies of any reference(s), applicant invites the Examiner to contact the undersigned. Documentation in the file wrapper of the instant application confirming the Examiner's consideration of the relevant reference(s) is respectfully requested.

The Examiner has required new corrected drawings in compliance with 37 CFR 1.121(d). Applicant submits that corrected drawing sheets are included herewith.

The Examiner has rejected Claims 1, 3-9, 12, 13, 15-21, 24, 25, 27-33 and 36 under 35 U.S.C. 103(a) as being unpatentable over Xu (U.S. Patent Application Publication No. 2002/0038339) in view of Tso (U.S. Patent No. 6,088,803). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to incorporate the subject matter of Claim 7 et al., amended independent Claim 1 to incorporate the subject matter of Claims 4 and 5, and amended independent Claims 13 and 25 to incorporate the subject matter of Claims 18 and 30, respectively.

With respect to the subject matter of Claim 4, as presently incorporated into independent Claim 1, the Examiner has relied on paragraph [0015] in Xu to make a prior art showing of applicant's claimed technique "wherein each device in the computer network is assigned an identifier, and the proxy device is assigned the same identifier as is assigned to the file storage device, the first interface being connectable to a communication infrastructure of the computer network to enable communication between the proxy device and said client devices, and the file storage device being connectable to the second interface such that the file storage device is only accessible by said client devices via said proxy device."

Applicant notes that such excerpt teaches that the "server 570 is operating in alias mode, [such that] the service IP address of W1 has been defined as one of server 570's IP addresses, so server 570 will accept those packets." However, applicant respectfully asserts that it is the packeting engine 500 in Xu that is connected between the client computer 520 and the server 570, and Xu does not teach that the packeting engine is assigned the same identifier as is assigned to the server. Instead, Xu only teaches that the server is assigned an IP address that is the same as the service IP address of W1, and not that a proxy device is assigned the same identifier as is assigned a file storage device, as claimed by applicant.

Furthermore, applicant emphasizes that the service IP address in Xu "is not the IP address of a physical system, [but] rather it is a routable IP address assigned to a customized service" (see [0111]). Thus, the server is Xu is assigned an IP address of a customized service, whereas applicant claims a "proxy device [that] is assigned the same identifier as is assigned to the file storage device" (emphasis added). In addition, in Xu, the "packeting engine 500 advertises that is it able to direct traffic from network 30 bound for service IP address W1" (see [0111]). Clearly, applicant's proxy device is not met by Xu's service IP address, since it is the packeting engine 500 in Xu that directs traffic to the service IP address.

With respect to the subject matter of Claim 5, as presently incorporated into independent Claim 1, the Examiner has relied on paragraph [0120] in Xu to make a prior art showing of applicant's claimed technique "wherein the second interface is configured to enable a plurality of file storage devices to be connected to the proxy device, each file storage device having a different identifier, and the proxy device being assigned multiple identifiers corresponding to the identifiers of the connected file storage devices, the first interface being configured to receive any access requests issued to one of said connected file storage devices."

Applicant respectfully asserts that such excerpt fails to teach that the "proxy device... [is] assigned multiple identifiers corresponding to the identifiers of the connected file storage devices." As argued above with respect to Claim 4, Xu only teaches that the servers are capable of having an alias corresponding to the service IP address W1. Clearly, such teaching does not meet applicant's specific claim language since applicant claims that the "proxy device...[is] assigned multiple identifiers corresponding to the identifiers of the connected file storage devices" (emphasis added).

With respect to the subject matter of Claim 7 et al., as presently incorporated into each of the independent claims, the Examiner has relied on the following excerpt from Tso to make a prior art showing of applicant's claimed technique "wherein the processing logic is responsive to configuration data to determine which malware scanning algorithms should be selected for a particular file, the proxy device further comprising a scanning engine to execute the malware scanning algorithms selected by the processing logic" (see the same or similar, but not identical language in each of the independent claims).

> "Referring to FIG. 3, as network device 4 is streaming the requested file to client device 12, it maintains a working copy of the transmitted portions (Steps 190, 220). Virus checker 5 performs virus checking (for example, using standard pattern scans) on the requested file as portions are received from content server 7, but again this processing does not delay the transfer of data to client device 12 (Step 150). If a virus is detected, network device 4 terminates both the transmission from content server 7 and the transmission to client device 1 (Steps 200, 210). Network device 4 may explicitly notify client device 1 that a virus was detected so that any previously-received portions of the requested file can be discarded, although in almost all existing file transfer applications, such as Web browsers and FTP (File Transfer Protocol) applications, an abnormal termination results in an automatic discard of any partially-transferred file." (Col. 3, lines 40-53)

Applicant notes that such excerpt only generally teaches that a virus checker "performs virus checking...on the requested file as portions are received." Applicant respectfully asserts that such general disclosure of virus checking all received portions of a file does not meet applicant's specific claim language, namely "configuration data

[that] determine[s] which malware scanning algorithms should be selected for a particular file" (emphasis added), as claimed.

With respect to the subject matter of Claim 18 et al., as presently incorporated into independent Claims 13 and 25, the Examiner has relied on paragraph [0016] in Xu to make a prior art showing of applicant's claimed technique "wherein each device in the computer network is assigned an identifier, the proxy device being assigned a unique identifier different to the identifier of the file storage device, the method comprising the steps of: connecting the client devices, the proxy device and the file storage device to a communication infrastructure of the computer network; configuring the client devices such that access requests issued by the client devices are routed to the proxy device; and configuring the file storage device to send processed access requests to the proxy device" (see the same or similar, but not identical language in each of the independent claims).

Specifically, the Examiner argues that Xu teaches that the proxy has a unique identifier compared to the storage device. Applicant notes, however, that Xu only teaches that the "packeting engine 500 receives packets on interface...with a destination IP address of service IP address W1 and service port of P1." However, nowhere in such excerpt does Xu even mention the packeting engine's IP address, let alone specifically disclose a "proxy device being assigned a unique identifier different to the identifier of the file storage device," as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 37-44 below, which are added for full consideration:

"wherein the processing logic determines whether the selected malware scanning algorithms are required to be run on the file before causing the selected malware scanning algorithms to be executed" (see Claim 37);

"wherein the determination is made according to additional configuration data specifying when scanning should be performed and the types of files that should be scanned" (see Claim 38);

"wherein for a plurality of file storage devices on the computer network, a plurality of proxy devices are provided such that each file storage device is associated with one of the proxy devices" (see Claim 39);

"wherein for a plurality of file storage devices on the computer network, the proxy device is associated with all of the file storage devices" (see Claim 40);

"wherein the proxy device is associated with all of the file storage devices when minimal scanning of files is performed" (see Claim 41);

"wherein a computer network administrator has direct access to the file storage device" (see Claim 42);

"wherein the plurality of client devices are allowed direct access to the file storage device if the proxy device fails" (see Claim 43); and

"wherein the predetermined attributes include a user name, a password of the user making the access request, a domain of the client device, an indication of the file to be accessed and an address of the client device" (see Claim 44).

Again, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P453/01.123.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100